# ESI CONSULTING

DIGITAL FORENSIC SERVICES



Richard D. Connor, Jr., Esq.
AccessData Certified Examiner
Certified Computer Examiner
Certified Forensic Computer
Examiner Digital Forensic
Certified Practitioner EnCase
Certified Examiner
IACIS Certified Mobile Device Examiner

May 12, 2022

Charles Swift
CLCMA
100 N. Central Expressway, Ste. 1010
Richardson, TX 75080

**Re: *United States v. Giampietro*, Case No. 2:19-cr-00013 (M.D. Tenn.)**

This is my Report in this matter based upon my examination and analysis to date of the items listed below. This report may be amended or supplemented if additional items are provided to me, or if additional examination or analysis is conducted.

**1. Items Examined**

**a.** Discovery provided by government.
**b.** Forensic images of seized devices.

**2. Results of Examination and Analysis**

**a. My Background**

I have practiced digital forensics since 2006, handling more than 1,600 matters and examining thousands of devices, primarily cell phones and computers. My practice involves examining and analyzing all types of software, hardware, and apps. I have testified in almost 200 cases, civil and criminal. My CV is attached

**b. Telegram App**

Telegram is a communication app, allowing users to send and receive messages, voice calls, and video calls. Telegram was founded in 2013 by two Russians, and was initially headquartered in Russia. It is now headquartered in Dubai. Telegram was created to challenge WhatsApp, with two

main features to distinguish it, user accounts could be accessed from multiple devices, and encryption. Telegram does not sell ads, and does not censor content. As of March 2018 there were about 200 million monthly users of Telegram. Telegram is very popular in countries where there is civil unrest against the government, such as Hong Kong. There are different methods of communicating on Telegram, channels, groups, chats, and secret chats.

**i. Channels**

Telegram channels are like groups where the user can create a channel and send messages which will be pushed to all followers of that channel. Channels are one way communications, the creator is the only person who can send messages to the channel followers. Followers cannot see who else is a follower of the channel. There is no limit to the number of followers. Channels can be public or private.

**ii. Groups**

Telegram groups are like most other group chat apps, where users can join a group, see who else is in the group, send messages to all members of the group, and read all messages posted by other members. Groups can have up to 200,000 members. Groups can be public or private.

**iii. Chats**

Telegram users can also chat, or message, other users directly, without joining a group or channel. Users can also delete chat messages from both the sender and recipient phones.

**iv. Secret Chats**

Secret chats use end to end encryption, and are not stored on any Telegram server. Secret chats can also be set to self-destruct a specified time after the message is opened by the recipient. Initially, a user could screenshot a secret chat without notifying the other participant. Many users did this, and Telegram now notifies the other participant if one takes a screenshot, and it is trying to prevent users from screenshotting secret chats. For example, I was not able to create a screenshot of a secret chat.

**c. Defendant's Use of Telegram**

Defendant first downloaded the Telegram app from the Google Play store on December 7, 2017. The Telegram app had been previously downloaded on defendant's Galaxy S5 on April 14, 2017. Defendant's Galaxy S8 phone contains about 160 chats with more than 3,400 individual messages. Some of these appear to be channels, and some appear to be chats. There are also

screenshots of chats on the phone. There are no secret chats on the phone, so they must have been set to self- destruct, and did self-destruct, as intended by Telegram. Thus the Telegram app deletes the secret chats, and once that happens, there is nothing for the user to delete.

Self-destructing secret chats are a feature of Telegram, and the parties to such a chat must agree to use the feature before engaging in such a chat. Secret chats cannot be forwarded, they cannot be saved, they can no longer be copied via screenshot[1]. In 2018, however, they could be copied by screenshot. The only data available are either screenshots taken by the defendant or the undercovers taken in 2018. If screenshots were not saved it is impossible to tell whether the secret chat feature was used and if it was used, who initiated the secret chat.

It is not possible to delete ones Telegram account from the phone app. A user can schedule to have an account deleted after a specified period of inactivity. What many users do, and what defendant may have done, is log out of one Telegram account, and then create a new Telegram account. This does not delete any Telegram data from the user's phone.

**d. Defendant's Phone**

I am aware that on October 16, 2018, Telegram messages were exchanged in which it was suggested the defendant deleted data from her cell phone. I have reviewed the cell phone and forensically, I have not seen any evidence or indication that the defendant wiped or reset her Galaxy S8 cell phone.

Sincerely,

Richard D. Connor, Jr., Esq. ACE CCE CFCE DFCP EnCE ICMDE

[1] My initial report indicate that Telegram accounts could not be copied by screenshot. That's statement was based on the Telegram App as it existed at the time of my report on August 20, 2020. However, the Telegram feature that prevented screenshots of secret chat messages, however, was not in use in 2018, and therefore a user could take a screenshot of a chat they were having in 2018.